Evolution of IoT devices: Future for Smart homes or a threat to your privacy and security?

Thomas Cunningham
dept.Science and technology
Bournemouth University
Dorset, Bournemouth
0000-0002-6664-7670

***Abstract*—For this paper, a topic of our choice related to cyber was allowed to be chosen in which we would have to write an academic about that topic. The paper will include aims and objectives which should be achieved from this problem space. Analysis of IoT devices will compare the pros and cons that these devices bring. This work discusses the uses of smart homes and the evolution of IoT along with the challenges they face and what the future could hold for them.**

Keywords- DDOS- Distributed Denial of Service attack, IoT, Man-In-The-Middle, Automation, Smart Homes

I. Introduction

This project is focused on IoT devices and whether they are a threat to our privacy and security. IoT is short for the internet of things and can be any device that has an IP address for internet connectivity that can communicate with other end devices. IoT devices could be a light bulb, speaker, smart fridge, smart TV, phone, computer and much more. In 2025, there is estimated to be around 75 billion devices connected to the internet. These devices bring large amounts of data that could be vulnerable to hackers. In the first six months of 2021, data showed that more than 1.5 billion attacks had occurred against IoT devices [1] IoT devices are used every day and with new technology being released people should understand the risks and threats that it could cause. The number of devices per household in the U.S has more than doubled from 2019 now being 25 devices compared to the previous number of 11[2].

II. Aims and objectives of this paper

A. ~Aims

This paper aims to explore IoT devices, how they have developed over recent years and if they are a threat to privacy and security.

B. Objectives

1- Investigate the history and evolution of IoT devices
2- Analyses IoT devices
3- Explore threats and attacks around IoT devices

III. History/ background of IoT devices

The main history of IoT began with the creation of the web in the late 1960s [3]. Sensor devices were then introduced in the 1980s along with the first linked gadget the Coca-Cola vending machine which was developed by university students and professors from Carnegie Melon university [3]. Small switches were combined into the machine that applied a type of web which checks whether the drinks were kept cold and were accessible or not [3]. The term IoT was first introduced in 1999 by Kevin Ashton where he described the term as 'technology that connects several devices with the help of RFID (Radio-frequency identification) tags for supply chain management [3].

At the start of the 21st century, several major developments happened in the IoT evolution. LG Electronics introduced a refrigerator that could connect to the internet and allowed its users to shop online and make videos calls. In 2005, a robot named Nabaztag was created which could tell the latest news, weather and stock market changes [3]. In 2008, the first international conference of the Internet of Things was held in Switzerland after the term came into widespread media and news outlets. RFIDs, short-range wireless communication and sensor networks were discussed. [3]

In 2011, IPv6 was released publicly as a network layer protocol that is central to IoT. IPv6 allows communication and data transfers to take place over the network. Since then, IoT devices have become widespread and have found their way into almost every industry from manufacturing, retail, oil & energy, agriculture and many more.

IV. How IoT works

Devices have built-in sensors and mini-computer processors that act on the data collected by the sensors via machine learning [4]. IoT devices are essentially minicomputers connected to the internet. There are four major components of the IoT ecosystem which are the following: Sensors/ devices, Connectivity, Data processing and the user interface. Once the data has been collected it is transferred to the cloud infrastructure (known as IoT platforms) [4]. However, to transfer that data, the devices will need a medium which is when connections like Bluetooth, WIFI and WAN come into play [4]. The mediums must be chosen wisely as the effectiveness of IoT security highly depends on the speed and availability of those mediums [4]. After the data has reached the cloud that data is then analysed so the right action can be taken [4]. The analyse could be as simple as the temperature of a device or a more complex situation such as when an intruder comes in and that device must identify it [4]. Once the data is analysed the action must be sent to the user either by an alert sound or notification sent to the IoT mobile app [4]. Once the alert is received the user will know the system works.

IoT has made its way into the businesses world but how does it work in those industries? In the education sector, IoT gives students greater access to everything from learning materials to communication with teachers, lecturers and other students. Since the start of Covid-19 IoT has massively helped the education sectors with the use of online learning. Remote learning would not have been possible without the help of IoT. In the retail sector, it has made its way via automated checkouts process, hand devices created to scan products, keep stock updates etc. In healthcare, IoT has enabled doctors to get real-time access to patient records data, store on the cloud and share it with other people [4]. IoT has managed to cut down waiting time and has allowed doctors and nurses to check the availability of certain hardware and equipment [4]. IoT has simplified the time it takes to identify illnesses and diseases and the right actions to take to reduce the risk [4]. IoT in the travel sector has enabled guests to receive real-time travel information on flights and has enhanced the travel experience for the tourist. For example, tourist-related companies and destinations can send location-specific information to customers which can improve the tourist's experience [5].

V. Smart homes

With IoT devices becoming normal in homes new devices are always being developed. A smart home refers to a convenient home setup where appliances and devices can be automatically controlled from anywhere in the home with an internet connection using a mobile or network device [7].

VI. Advanatges of iot devices

One of the main benefits IoT devices bring is how easy it can be to stay connected and communicate with other people. People can keep in touch with long-distance friends and family by sending a message or having an audio/ video call. Safety is another element that IoT devices can have on households. Devices such as CCTV cameras and home security systems are put in place where the user can receive alerts of movement or if their doorbell is pressed via their phone. Personal assistance could be provided by IoT apps for users such as alerts reminding the user when to take certain medicines or have reminders for doctor's appointments etc [9]. Information is easily accessible whether that is searching for it online or having data stored on your device. For example, work rotas could be shared online saving you from going to work to find out when your next shift is. The ease of use and setting up IoT devices is another benefit as it minimizes human activity. For example, communicating with other people can be done online instead of face to face which could result in them getting more tasks done at home or elsewhere. Transferring data packets over a connected network saves time and money thanks to IoT [10]. Automation helps boost the quality of services and reduced human interaction. Reduced human interaction results in lower operating costs for businesses as it could take 5 people to do the one task that a robot is performing also resulting in lower heating requirements in automated operations [11].

VII. Disadvantages of IoT attacks

Data breaches are a huge problem for IoT systems especially with companies as their clients could lose trust in them if a massive breach has occurred.

In 2020, there were around 1001 data breaches in the U.S with over 155.8 million records being affected by data exposure [12].

Laws and regulations are a problem for companies such as GDPR as the company has failed its integrity and confidentiality of the user's data. This can cause financial strain on the company which often leads to them going bankrupt and closing. The 7 principles of GDPR are the following: lawfulness/ fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and accountability. GDPR is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the EU [13].

Misuse of information and devices is another problem that occurs. If hackers gain access to a system, they could change settings on IoT devices from as little as the colour of an LED light or what sets the fridge temperature is. However, more serious cases could include turning off or taking over home security systems and/ or broadcasting them to other people. IoT systems rely heavily on an internet connection so without it they are less usable or do not function at all. For example, if you want to set up virtual assistance such as an Amazon Alexa you must connect it to a WIFI network otherwise it will not work. People rely too much on technology and almost become dependent on it for daily tasks such as turning a light switch on by your phone or having a virtual assistant to answer your questions. Other examples of technology dependency could be using a device to control your central heating system or to turn your tv on or off. Automation can bring benefits to the economy however, there are many problems it causes such as unemployment. For example, with smart surveillance cameras, there is not a need for a security guard Another example could be machined replacing people for work in factors such as food factors where most places use machines to mix prepare food. This results in less skilled people becoming unemployed.

VIII. Privacy and security concerns

In 2018, a US casino was hacked through a fish tank [14]. An internet-connected thermometer inside the tank was used as an entry point to infiltrate the casino's entire system and extract clients' data [14]. Privacy is also an issue with the audio-based device that can listen to our daily conversations. Devices such as Amazon Alexa record recordings when the device is spoken to however, there have been serval reports where 'Alexa' have begun recording by mistake [14]. Other concerns are that Amazon employees listen to recordings from 'Alexa' to improve the quality of service [14]. Working from home has its benefits and problems however, with Covid-19 more people have started to work from home and with remote access has meant the 'average office' is now full of more internet-connected devices [14]. Employees using their home WI-FI network to log onto work devices could be putting corporate networks at risk. Insufficient physical security is another issue. If hackers have access to a physical device, they can open the device and attack the hardware [14]. An example of this could be if someone breaks into your house, they can access the physical device exploit malware on that device and then gain access to other devices connected to the network. The number of devices connected to the internet will always grow increasing the number of ways our devices can be hacked or exploited and having mentioned at the start of this paper that 1.5 billion attacks occurred against IoT devices in 2021 that number is certain to accelerate in into 2022.

IX. Types of attacks that have occurred

IoT devices face many attacks which some have previously been mentioned such as the compromise of smart home surveillance. Other reports found that hackers have taken over smart home systems by playing music and even started talking to them from a camera in their kitchen whilst changing the temperature of the room to 90+ degrees. Smart bulbs are another device hackers have gained access to via sending an infrared signal to other infrared bulbs. Once they have gained access hackers then, can view and breach other devices connected to the network. Smart TVs are another popular device that is breached [15]. Once hackers have access, they can control the volume and channel controls but could listen to your conversation or even watch you if the TV has a built-in camera [15]. The most common attacks that have occurred are botnet attacks, which is when hackers remotely take control of a system via exploiting malware. Social engineering is another common attack that occurs when the attacker manipulates people into giving up confidential information. Denial of service attacks happen through a botnet and causes a system overload by programming devices to request at the same time [16]. Data and identity theft is another frequent attack with lots of data being available online via social media and other websites. Once hackers have gained access to a device that has social media accounts, they have all that information made available for them to just copy or sell to other third parties which then is copied. Man-in-the-middle (MitM) is another concern, especially with IoT devices. When a device communicates using plain text all information is being exchanged with a client device or backend service it can be obtained by a (MitM) [16].

X. Challenges ahead for IoT devices

No one knows what the future holds for IoT and with the popularity forever increasing it could cause further issues for users and developers. Current issues for IoT devices are still occurring such as security and privacy issues, lack of regulation about IoT and compatibility issues. Even though the technology is evolving, and security issues are being fixed, cybercriminals will continue to find ways to attack systems and devices. Companies need to start prioritising security in these devices and not after they have been exploited.

XI. Future predictions for IoT

People have predicted many outcomes and possibilities for the future of IoT devices: Cities will become “smart”, Artificial intelligence will continue to grow, the arrival of 5G will continue to grow and fuel IoT growth. The metaverse interlocks with IoT.

XII. Conclusion

In conclusion, I hope this paper has given people an insight into how dangerous and vulnerable IoT devices in your home could be, however, they also bring many positive impacts into your Smart home such as improved security systems.

References

[1] D. Paul, "IoT devices see more than 1.5bn cyberattacks so far this year", *Digit*, 2021. [Online]. Available: https://digit.fyi/iot-security-kaspersky-research attacks/#:~:text=Data%20showed%20that%20more%20than,first%20six%20months%20of%2020. [Accessed: 07- Nov- 2021].

[2] P. Britt, "Report: Connected Devices Have More Than Doubled Since 2019 - Telecompetitor", *Telecompetitor.com*, 2021. [Online]. Available: https://www.telecompetitor.com/report-connected-devices-have-more-than-doubled-since-2019. [Accessed: 08- Nov- 2021].

[3] S. Khvoynitskaya, "The IoT history and future - Itransition", *Itransition.com*, 2022. [Online]. Available: https://www.itransition.com/blog/iot-history. [Accessed: 12- Jan-2022].

[4] S. Srivastava, "What is Internet of Things and How is it Affecting Us?", *Appinventiv*, 2021. [Online]. Available: https://appinventiv.com/blog/what-is-internet-of-things/. [Accessed: 12- Jan- 2022].

[5] GlobalData Thematic Research, "Internet of Things (IoT) in Travel and Tourism: Industry trends", *Hotel Management Network*, 2021. [Online]. Available: https://www.hotelmanagement-network.com/comment/internet-of-things-iot-travel-tourism-industry-trends/. [Accessed: 12- Jan- 2022].

[6] M. Bansal, M. Nanda and M. Husain, "2021 6th International Conference on Inventive Computation Technologies (ICICT)", *An overview of IoT based smart homes (ICICT*, 2021. Available: https://ieeexplore.ieee.org/abstract/document/9358665/citations. [Accessed 12 January 2022].

[7] A. Hayes, "What is a Smart Home", *Investopedia*, 2022. [Online]. Available: https://www.investopedia.com/terms/s/smart-home.asp#:~:text=A%20smart%20home%20allows%20homeowners,with%20convenience%20and%20cost%20savings. [Accessed: 12-Jan- 2022].

[8] C. Paul, A. Ganesh and C. Sunitha, "An overview of IoT based smart homes", *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, 2018. Available: https://ieeexplore.ieee.org/abstract/document/8398858/authors. [Accessed 12 January 2022].

[9] guduruaishwarya09, "Advantages and Disadvantages of IoT - GeeksforGeeks", *GeeksforGeeks*, 2021. [Online]. Available: https://www.geeksforgeeks.org/advantages-and-disadvantages-of-iot. [Accessed: 07- Nov- 2021]

[10] Redalkem, "Advantages and Disadvantages of Internet of Things! - RedAlkemi", *Redalkemi.com*, 2018. [Online]. Available: https://www.redalkemi.com/blog/post/pros-cons-of-internet-of-things. [Accessed: 08- Nov- 2021].

[11] Productivity Inc, "Benefits of Automation | Robotic Manufacturing Automation, Robotics & Automation Solutions | Productivity Inc", *Productivity Inc*, 2022. [Online]. Available: https://www.productivity.com/benefits-of-automation. [Accessed: 07-Nov- 2021].

[12] . Johnson, "U.S. data breaches and exposed records 2020 | Statista", *Statista*, 2021. [Online]. Available: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/#:~:text=In%202020%2C%20the%20number%20of,%2Dthan%2Dadequate%20information%20security. [Accessed: 13- Jan-2022].

[13] . Frankfenfield, "General Data Protection Regulation (GDPR)", *Investopedia*, 2020. [Online]. Available: https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp. [Accessed: 12- Jan- 2022]

[14] C. Hopping, "IoT privacy and security concerns", *Itpro.co.uk*, 2021. [Online]. Available: https://www.itpro.co.uk/security/28086/iot-privacy-security-concerns. [Accessed: 12- Jan- 2022].

[15]] R. Srinivas, "10 IoT Security Incidents That Make You Feel Less Secure", *CISO MAG | Cyber Security Magazine*, 2020. [Online]. Available: https://cisomag.eccouncil.org/10-iot-security-incidents-that-make-you-feel-less-secure. [Accessed: 08- Nov- 2021].

[16] L. Toms, "5 Common Cyber Attacks in the IoT", *GlobalSign GMO Internet, Inc.*, 2016. [Online]. Available: https://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot. [Accessed: 07- Nov- 2021].

[17] S. Langkemper, "The Most Important Security Problems with IoT Devices", *The Most Important Security Problems with IoT Devices*. [Online]. Available: https://www.eurofins-cybersecurity.com/news/security-problems-iot-devices/. [Accessed: 12- Jan- 2022].

[18] K. Began, "5 challenges still facing the Internet of Things | IoT Now News & Reports", *IoT Now News - How to run an IoT enabled business*. [Online]. Available: https://www.iot-now.com/2020/. [Accessed: 12- Jan- 2022].

[19] O. Martynova, "The Future of IoT: Innovations to Expect in the New Decade - Intellias", *Intellias*, 2020. [Online]. Available: https://intellias.com/the-future-of-iot/. [Accessed: 12- Jan- 2022].

[20] S. Symanovich, "The Future of IoT: 10 Predictions about the Internet of Things | Norton", *Us.norton.com*, 2019. [Online]. Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html. [Accessed: 12- Jan- 2022].